Service Shell

Modifying User Account Setup and Access

73400016A-EN Rev A

2003-12-02

Creo Inc.
3700 Gilmore Way
Burnaby, BC
Canada V5G 4M1
(604) 451-2700

Copyright 2003 Creo Inc. All rights reserved.

This page intentionally left blank.

Revision History

Revision	Date	Author	Comments
Draft	2001	Omar Jaber	Initial draft
1.0	2002	Michael Joy/Omar Jaber	Revised initial draft and incorporated changes recommended by Michael Joy.
2.0	Nov. 4, 2003	Omar Jaber	Updated document for Service Shell 2.5
2.1	Nov. 10, 2003	Brian Holness	Edit, check for procedure accuracy, correct where necessary
2.2	Nov. 27, 2003	Brian Holness	Update, PDF

This page intentionally left blank.

CONTENTS

Revision History i

1. Introduction 1
   1.1 Service Shell Components & Required Privileges 1
   1.2 Customer Account Specifications 3
   1.3 Administrative Account 3
      1.3.1 User Rights: 3
      1.3.2 Service Shell Changes: 3
   1.4 Power User Account 3
      1.4.1 User Rights: 3
      1.4.2 Directions for disabling the Add/Remove program control panel 4
      1.4.3 Service Shell Changes: 5
   1.5 Normal User Account 5
      1.5.1 User Rights: 5
      1.5.2 Service Shell Changes: 6
   1.6 Summary 6

This page intentionally left blank.

1. INTRODUCTION

The purpose of this document is to clarify Service Shell requirements related to account security. Additional workarounds for requirements not currently fulfilled by Service Shell are also covered. The information applies to all Service Shell versions up to and including 2.5. The document assumes that the reader understands the Service Shell client/server model and is familiar with Microsoft® Windows NT security. Finally, the solutions in this document assume that Service Shell and Print Console are the only Creo software programs running on the workstation.

1.1 Service Shell Components and Required Privileges

This section lists Service Shell components and their required system privileges. The information is true for all Service Shell versions prior to and including Service Shell 2.5.

Component	Type	Required Privileges
ServiceMonitor.exe	Server-side Windows NT, 2000, XP application	ServiceMonitor.exe adds LaunchServiceHost service to Windows NT Service Control Manager (SCM) table if it does not exist. It also provides an interface to start, stop, and configure Service Host. Unless the security templates for the system are customized, the adding and removing of services to and from SCM table requires Administrative account. Therefore, this application requires Administrative privileges.
LaunchServiceHost.exe	Server-side Windows NT, 2000, XP Service	This is an OS service — it must be installed under a Power User or Administrative account. If the service is installed to run automatically (default setting in Service Shell 2.4 and later), then a User account should suffice. Otherwise, you need a Power User or Administrative account to start and stop the service.
CreoDeviceServer.exe	Server-side Windows NT, 2000, XP	User

Component	Type	Required Privileges
	application	
LogViewServer.exe	Server-side Windows NT, 2000, XP application	User
Diagnostics programs	Server-side Windows NT, 2000, XP applications	User
Service.exe	Server-side Windows NT, 2000, XP application	**Service.exe**, modifies some registry keys under Service Shell the registry tree and uses a raw socket to ping the host machine. Unless the security templates are customized, modifying a registry and opening a raw socket requires a Power User account. Therefore, this application requires a Power User privileges.

Note: Service Shell 2.5 requires an account with administrative privileges to run all of its components.

1.2 Customer Account Requirements

These are the account requirements provided by CTP Product Specialist, Eric Nelson, based on customer feedback.

- User can't change password
- User pass-word never expires
- User can't add or remove programs
- User can't modify the system registry

The first two requirements can easily be achieved by configuring the user account password from Microsoft Management Console (MMC). The remaining two specifications are more problematic since they conflict with Service Shell requirements. Sections 1.3, 1.4, and 1.5 propose various account setups to satisfy both customer and Service Shell requirements.

1.3 Administrative Account

1.3.1 User Rights

A user with an Administrative account can modify anything (including the system registry) access any folder on the system, or change any object membership/ownership.

1.3.2 Service Shell Changes

If Service Shell is run from an administrative account, then there are no changes required to run version 2.5 release and later.

1.4 Power User Account

1.4.1 User Rights

A user with a Power User account can add and remove programs that don’t modify the system registry, modify any application registry key under **HKEY_LOCAL_MACHINE**, and create a user account with similar or lower user rights.

Although the user can add or remove programs, the programs added cannot modify the system registry, which ensures that the system will continue to function.

To disable the Service Shell installer for this account type:

1. Logon to the workstation as an administrator.
2. Disable the Windows installer for all users except for the Administrator.

Note: This will not stop users from copying executables to the hard drive, but will prevent them from installing programs that require registering components or modifying system folders.

3. To disable the Windows installer:

   a) Select **Start** > **Run**, and type `gpedit.msc` in the open box. Press ENTER.

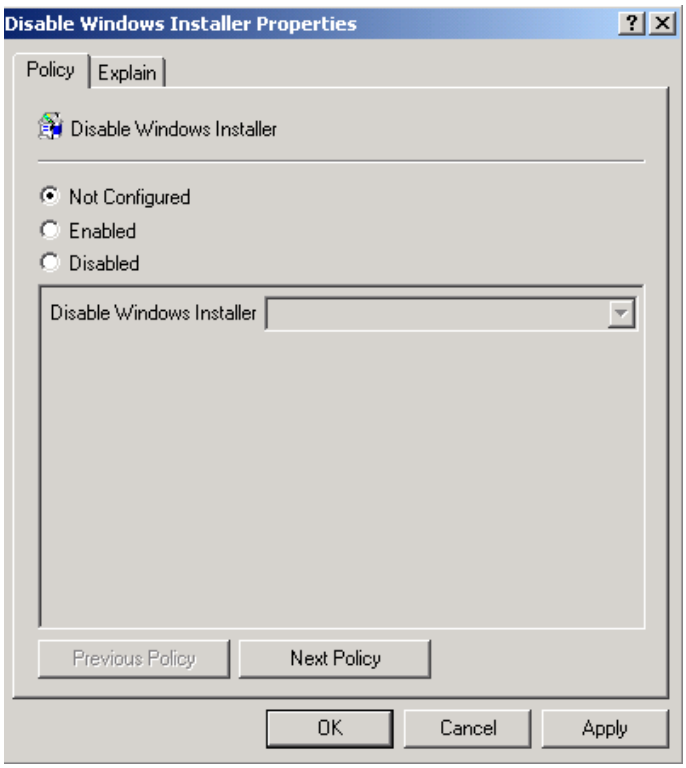
   b) Click + to expand the **Computer Configuration** tree.

   c) Click + to expand **Administrative Templates**.

   d) Click + to expand **Windows Components**.

   e) Click **Windows Installer**. A new window opens.

   f) On the right-hand pane, double-click **Disable Windows Installer**. The **Disable Windows Installer Properties** dialog box appears.



   g) Select the **Enabled** radio option.

   h) In the **Disable Windows Installer** list, select **Always** (recommended) or **Non Managed Apps only**.

1.4.2 Disabling the Add/Remove program control panel

1. Select **Start** > **Run**, and type `gpedit.msc` in the open box. Press ENTER.

2. Click + to expand the **User Configuration** tree.
3. Click + to expand **Administrative Templates.**
4. Click + to expand **Control Panel.**
5. Click **Add/Remove Programs**. A new window opens.
6. Double-click **Remove Add/Remove Programs Programs**.
7. Select the **Enabled** option.
8. Click **Apply**.

These changes have no impact on the Administrator account. Now a user with a Power User account can only add programs that a Normal User can add (programs that don't require system registry access, components registration, and use of Windows installer).

1.4.3 Service Shell Changes

If you are running Service Shell from a Power User account, **ServiceMonitor.exe** will not be able to add and remove the **LaunchServiceHost.exe** service, but it can start and stop the service. A Power User account will satisfy all of the Service Shell account requirements except for those of **ServiceMonitor.exe**. Service Shell 2.5 and prior versions require a Power User account. However, the following two changes to Service Shell will drop **ServiceMonitor.exe** requirements from an Administrator to a Power User account, which will ensure that Service Shell will run under a Power User account.

- Service Shell installer should add and remove **LaunchServiceHost.exe** service when Service Shell is installed and removed.
- **SeviceMonitor.exe** should only start and stop **LaunchServiceHost.exe** service at startup and shutdown.

1.5 Normal User Account

1.5.1 User Rights

The Normal User account has rights very similar to the Power User account, with the following exceptions:

- Normal Users can only add programs that don't require system registry access, components registration, or use of Windows installer.
- Normal Users cannot add user accounts
- Normal Users cannot perform system time updates
- Normal Users cannot create or delete new keys under **HKEY_LOCAL_MACHINE**

- Normal Users cannot start and stop Windows NT or 2000 service

A Normal User account fails to satisfy **LaunchServiceHost.exe**, **ServiceMonitor.exe**, and **Service.exe** requirements, and it provides no more security to the system that the modified Power Account as described in Section 1.4.

1.5.2 Service Shell Changes

Service Host can be modified to run under a Normal User account, but the changes may restrict future Service Shell features from functioning in this mode.

1. Logon to the workstation as an Administrator.
2. Install **Service Host**.
3. Remove **Service Host** from the Windows startup menu.
4. Select **Start** > **Run** and browse to the application **LaunchServiceHost.exe** under **ServiceShell\bin** directory. Click **Open.**
5. Add the option **–i** to the front of the application name and click **OK.**
6. Go to **Administrative Tools > Services**, and ensure that **LaunchServiceHost** is there and that it is configured to start automatically.
7. Log off, and log on as any other user. Start Task Manager and ensure that the processes **CreoDeviceServe.exe** and **LogViewServ.exe** are running.

1.6 Summary

Although some parts of Service Shell Host and Client can be set up to run under any account, Service Shell currently requires Administrator access to run all of its components.

With some additional development work and some onsite configuration, Service Shell can be made to run under a Power User account, and satisfy all the customer requirements. This is the recommended approach should the user accounts settings need to be modified.

Service Shell can also be made to run under a Normal User account. However, this requires some more complicated onsite configuration and may limit future Service Shell features from functioning in this mode. This approach should not be taken unless absolutely necessary.